Safeguard Your Business without Compromising Productivity

HOW TO OPTIMIZE SECURITY AND PRODUCTIVITY TO REALIZE BETTER BUSINESS OUTCOMES

In an age where the future of work looks more remote than ever, it's time to rethink how we not only compliantly protect customer information, but the critical data employees create and use as well. However, in doing so we must also actively remember the value of employee productivity and experience.

In fact, in a recent CIO COVID-19 Impact Study, 55% of enterprises expressed that optimizing the employee digital experience has increased in priority for their business since the pandemic outbreak. It's likely because businesses realize that to ensure positive business outcomes, they must empower employees to be productive no matter where they are working – while also ensuring security and compliance.

It's these three priority pillars – security, productivity and outcomes – that must be mindfully balanced throughout any comprehensive IT framework. Without proper security protections and compliance adherence, the business is put at unnecessary risk. But this should never come at the expense of the employee experience, which is directly aligned with productivity. And combined, security and productivity have a direct impact on enabling successful business outcomes in support of a company's future viability.

[1] CIO COVID-19 Impact Study, April 2020

ipm SUCCESS BRIEF

IPM migrated 800 users to Office 365 and Teams across the US, UK and France for a leading **Private Equity and Asset Management Firm**, improving email uptime and providing new productivity tools for users.

Let's consider how these three core elements, security, productivity and outcomes, should be addressed across your IT framework in our new era of a more remote and agile workforce.

OPTIMIZING HYBRID ENVIRONMENTS AND WORK

Not only are today's IT infrastructures increasingly adopting a hybrid cloud approach to their environment, employees too are embracing a hybrid style to their digital work as a result of the COVID-19 pandemic. While some employees will evolve back into the office, some may remain at home, while others still may find a new state of normal with a hybrid home/office. It's a clear example of how our new, more agile work world must better support data and application access for employees anywhere they wish to work, at any time and on any device.

Security in the Cloud

Consider the fact that 21% of organizations[2] have adopted a cloud-first strategy, up from 16% in 2018, mainly to make data more available for remote workers (26%) and to improve cost efficiency (30%). This trend will only grow, pointing to an increased need to address cloud security along with continued attention to on-premises infrastructure.

While migrating on-premises workloads to the cloud many security controls can be inherited and adapted to cloud infrastructure, but additional security considerations must also be addressed. This requires thoughtful design and mapping of existing on-premises security processes and a full understanding of the cloud's shared responsibility model. You'll need to establish an outline of the elements of security supplied by your cloud provider – such as protections for cloud hardware, compute and storage – and what you must secure yourself, including the user data, platforms, applications, identity access and firewall configuration.

One useful resource for Microsoft 365 users, specifically, is the Microsoft Secure Score[3] which is a measurement of an organization's security posture, with a higher number indicating more improvement actions have been taken. The tool provides a centralized dashboard in the Microsoft 365 security center where you can monitor and work on the security of Microsoft 365 identities, data, apps, devices and infrastructure. It helps organizations report on their current security posture while making recommendations that can be strategically applied by trusted IT consultants on how to improve security through discoverability, visibility, guidance and control.

55% of enterprises expressed that optimizing the employee digital experience has increased in priority for their business since the pandemic outbreak.

CIO Covid-19 Impact Study, April 2020

Empowering the Remote Worker

As workloads, including both applications and data, shift to the cloud, there must be close attention paid to how the cloud can best enable remote workers. Security practices can't limit user productivity. The risk is that you may defeat your own best cybersecurity processes and drive users to unapproved shadow IT services to support their remote work activities. Be sure to balance security practices carefully while supporting the availability and accessibility needs of offsite users.

[2] 2019 Netwrix Cloud Data Security Report
[3] Microsoft Secure Score How-to Guide

A recent study by Oxford Economics[4] shows that while 61% of IT organizations are building support for off-site environments, just 59% are assuring that data is securely available to relevant users. Even worse, only 31% have policies to safeguard sensitive information when contract workers leave. This demonstrates a key point. Data needs to be both secured and available – but only to those that truly need it to get their job done. Further, you can't forget the risk of contract workers or remote employees once they exit their roles. You need to have best practices to both onboard and offboard workers securely so that they may remain productive without adding risk exposure.

Only 31% of IT organizations have policies to safeguard sensitive information when contract workers leave.

Oxford Economics, Building the Digital Workplace

One example of a way organizations are improving user experience is through the use of Microsoft Intune and Windows Autopilot. These solutions help to build and maintain a customized operating system image to simplify what has traditionally been a very time-consuming process. Using these tools, you can literally drop-ship a brand-new laptop or device to remote users. Then, right out of the box, they can power it on immediately to a predetermined set up process that will automate security policies as well as control profiles, applications and more. It's a powerful option during this time of unprecedented remote workforces, giving users the immediate access they need to be productive, while ensuring security and policy control practices are properly followed.

Optimizing Business Availability

As you address the security and productivity requirements of today's agile, work from anywhere, worker, it's advised to also consider how to balance them to support business availability. The traditional "disaster," including hurricanes or fires, has now evolved to include ransomware attacks and even human viruses. Each can impact business continuity in different ways, but all require the need to be prepared. This need is equally important in the cloud as it is on premises – particularly given the fact that nearly half of IT organizations[5] store personally identifying information (PII) of customers and employees in the cloud.

Recovery strategies are of acute importance to assuring business continuity in the face of any type of disaster – particularly given the fact that IT downtime can cost up to $5,600 per minute.[6] Be sure to first outline the critical data that you need to protect, how you are ensuring its recovery, the processes used to thwart cybersecurity breaches and what practices and policies you need to follow to ensure compliance with regulatory requirements. Each of these works together to ensure your security and recovery posture will support a resilient business, with the acceptable availability to support your desired business outcomes.

Adopt a Shared Responsibility Model for Complete Cloud Data Security

Read five key considerations to build a more secure cloud infrastructure.

Download PDF

Striking the delicate balance between security, user productivity and business availability can be tricky, but vital. The process requires a deep understanding of your business goals, user workflows and desired security and compliance profile. To ensure the best outcomes it is often helpful to engage an expert consultant that has the field-proven experience and solution knowledge to best align your goals strategically with the technologies and approaches that will delivered the desired results.

[4] Oxford Economics, Building the Digital Workplace
[5] 2019 Netwrix Cloud Data Security Report
[6] Garter, The Cost of Downtime

ipm SUCCESS BRIEF

More than 1,000 users upgraded to Windows 10 on-time and on-budget at a **Mid-sized Financial Services Company** using IPM Project Management and Subject Matter Experts.

PROTECTING CLOUD AND DISTRIBUTED DATA

Today's remote workforce also poses new data protection challenges. Cloud-based collaboration and office productivity platforms, like Microsoft Office 365, are being used at an all-time record high – supporting as many as 200 million monthly active Office 365 business users.[7] That means new thinking must be given to how these platforms are both protected and compliantly managed. With growing cybersecurity risks and stringent regulations including GDPR, CCPA, PCI DSS and HIPAA on the rise, the handling, collection and storage of cloud-based data can't be ignored. While Office 365 is indeed a secure and empowering solution for businesses with remote users in particular, it doesn't offer the native backup and recovery services you likely need to assure business continuity and preserve data in the event of a disaster. It also prohibits you from retaining data according to industry regulations.

In many cases, it's necessary to supplement cloud-based applications with a cloud-aware data protection solution and strategy that will help you protect data, prevent risk and simplify compliance. Opt for solutions that will deliver policy-based backup, recovery, search and discovery for the cloud-based applications your employees use. This will ensure that you are recovery ready, while giving your compliance teams the tools they need to respond to specific data discovery requests via self service in many cases.

When it comes to data protection, inaction can result in devastating data breaches with multi-million-dollar consequences, including downtime and potential fines. Be certain that with the increasing amount of cloud-based data, you refine your backup and recovery strategy to best protect data in the cloud, as well as on premises. Experienced IT consultants can be unbelievably valuable in this process by helping to apply data protection best practices that will ensure the business continuity that aligns with your operational requirements. It's a risk your business can't afford to get wrong.

ASSURING EMPLOYEE PRODUCTIVITY AND ENGAGEMENT

You've built and optimized your security framework, effectively migrated key workloads to the cloud and taken action to ensure that data is available, accessible and protected for the workers that need it. Outstanding! But now, how do you truly know that they are achieving the experience and productivity they require?

The productivity gap—said to be as costly as $2.7 trillion—is dragging down the success of technology implementation on business outcomes.

Citrix, The Growing U.S. IT Productivity Gap

Understanding user experience (UX) is critical to ensure employees have what they need and value, while being mindful of usability, accessibility and perhaps most of all, time. A Citrix report[8] on the growing U.S. IT productivity gap has shown that productivity growth has slowed down, despite a rising investment in IT. The cause? Increased complexity, acceleration of security attacks and rapid data growth were named among the top issues. This productivity gap – said to be as costly as $2.7 trillion – is dragging down the success of technology implementation on business outcomes.

One way to overcome this productivity gap is to have greater visibility and insight into the true performance of employee devices and the applications they access. By using performance and availability testing techniques, you can proactively determine when performance and availability are at risk and help prevent the loss of productivity

[7] Venture Beat, "Microsoft 365 Bundles Office 365 with AI and Cloud-powered Features," March 30, 2020

[8] Citrix, The Growing U.S. IT Productivity Gap

and engagement. As a result, you'll help the business realize greater employee efficiency and output, employees will remain more content and business availability will remain high.

It's important to note that, during this time where employees are working remotely in larger numbers than ever, many may be accessing business data with both personal and work-provided devices. It's vital to support this worker productivity requirement, but you still must ensure that business data is secure. Select IT consultants and solution providers that understand this very crucial balance so that you can enable the secure, productive business outcomes that will help you thrive.

DRIVING BETTER OUTCOMES WITH PURPOSE

By clearly focusing on the interdependency of security and productivity on business outcomes, you can ensure that you are building the IT framework that will best support your company priorities and the employees that are tasked with achieving them. By working together with an expert IT consultant to look at each stage of the IT lifecycle and how it engages with security and productivity to achieve desired business goals, you'll benefit from a productive workforce that can be secure and engaged from anywhere.

Protecting Your Remote Workers' Data

Discover the best practices to ensure that the remote workforce can be productive in a secure data environment.

Download PDF

IPM is a US-based IT Consulting partner with 35 years' experience planning, deploying and supporting all aspects of IT infrastructure for our customers. We enable customers to transition to the cloud by selecting the right cloud model for their goals. We partner with best of breed technology partners to help organizations collaborate and be more productive, wherever they are working. Security is the cornerstone of all of the solutions we develop with a special focus on highly regulated industries and compliance. With strong partnerships and certification at the highest levels with partners including Microsoft, DellEMC, Citrix, VMware and Amazon, we have the ability to create and deliver secure IT solutions to meet your business needs and project budgets.

ipm

151 W. 30th Street, 8th Floor | New York, NY 10001

646.421.2801 | www.ipm.com | services@ipm.com